Edición 19 Febrero 2026

CIBER E-DEA

Boletín de Seguridad

7 filtraciones y exposiciones de datos que debe conocer (enero de 2026)

NUEVO ATAQUE DE CLICKFIX QUE ABUSA DE NSLOOKUP PARA RECUPERAR LA CARGA ÚTIL DE POWERSHELL A TRAVÉS DE DNS

La Guerra Híbrida llega a la Nieve: El Sabotaje Ruso Frustrado en los Juegos de Milán-Cortina 2026

Cómo proteger a las organizaciones durante los Juegos Olímpicos de Invierno, según los CISO

Vulnerabilidades destacadas

Ciber Incidentes en Colombia y en el mundo

e-dea NETWORKS | CYBER SECURITY

Great Place To Work. Certificada NOV 2024 - NOV 2025 COL
icontec ISO 9001 CO-SC-CER890596
icontec ISO 45001 CO-ST-CER890599
icontec ISO / IEC 27001 CO-SI-2001607
IQNET CERTIFIED MANAGEMENT SYSTEM

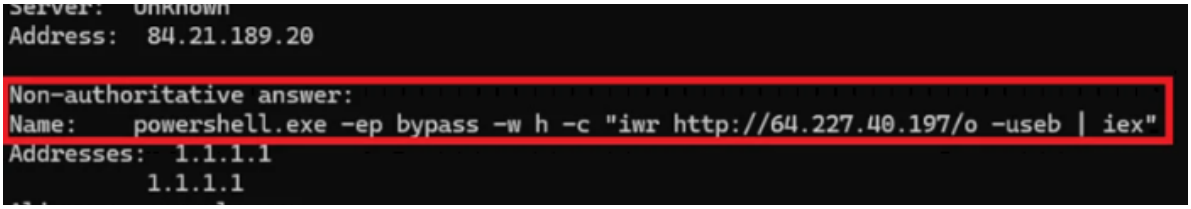
7 filtraciones y exposiciones de datos que debe conocer (enero de 2026)

El panorama de la ciberseguridad al inicio de 2026 marca un cambio en las tácticas delictivas. Según informes recientes, aunque el número total de víctimas ha disminuido, la cantidad de ataques ha alcanzado un récord histórico. Esto demuestra que los cibercriminales han abandonado operaciones de precisión dirigidas a activos de alto valor y propiedad intelectual.

1. Ataque Estructural a Target: La compañía sufrió el robo de 860 GB de código fuente y documentación técnica. A diferencia de los robos de datos financieros, este incidente compromete la infraestructura de seguridad a largo plazo de la empresa al exponer su arquitectura interna de software.
2. Brecha en el "Hogar de los Hackers": BreachForums, una de las plataformas más conocidas de cibercrimen, fue víctima de su propio sistema. Se filtraron metadatos de más de 324,000 usuarios, revelando identidades, correos e IPs de actores que operaban en la clandestinidad.
3. Vulnerabilidades Gubernamentales (ICE y DHS): El sector público se vio gravemente afectado. El ICE expuso accidentalmente datos de más de 2,000 agentes, facilitando un ciberataque posterior. Por su parte, el Departamento de Servicios Humanos (DHS) reportó incidentes que afectaron a un millón de personas, evidenciando que los errores humanos y los accesos no autorizados internos siguen siendo una debilidad crítica en las instituciones.
4. Crisis en el Sector Educativo (Universidad Monroe): Se confirmó una filtración masiva de datos sensibles (Seguridad Social, pasaportes e historiales médicos) de 320,000 personas. El caso destaca por la latencia del ataque, ocurrido en 2024 pero notificado hasta ahora, lo que ha generado severas repercusiones legales.
5. Exposición Masiva en el Sector Retail (Under Armour): Se hicieron públicos los datos de 72 millones de clientes. Aunque el robo ocurrió a finales de 2025, la disponibilidad de correos y registros de compra en foros de hacking aumenta exponencialmente el riesgo de campañas de phishing hiper-dirigido.
6. El Megahallazgo de Credenciales: El investigador Jeremiah Fowler descubrió una base de datos expuesta de 96 GB con 149 millones de registros. Este hallazgo es alarmante por su escala: incluye millones de cuentas de Gmail, Facebook, Instagram y Netflix, permitiendo en muchos casos el acceso directo a información bancaria y financiera de usuarios globales.

NUEVO ATAQUE DE CLICKFIX QUE ABUSA DE NSLOOKUP PARA RECUPERAR LA CARGA ÚTIL DE POWERSHELL A TRAVÉS DE DNS

Una nueva variante de los ataques ClickFix está utilizando consultas DNS para distribuir malware, siendo el primer caso conocido en el que este canal se emplea en estas campañas. Los atacantes continúan engañando a los usuarios mediante ingeniería social para que ejecuten comandos maliciosos, pero ahora recuperan la carga útil de una segunda etapa desde servidores DNS controlados por ellos, lo que dificulta su detección.



Las consultas DNS entregan un script de PowerShell malicioso

En una campaña reciente observada por Microsoft, los ataques ClickFix instruyen a las víctimas a ejecutar un comando nslookup que consulta un servidor DNS controlado por el atacante en lugar del predeterminado. La respuesta de esa consulta incluye un script malicioso de PowerShell, el cual se ejecuta para instalar malware.

Los investigadores también detectaron una técnica de evasión en la que el comando realiza una búsqueda DNS personalizada y extrae la carga útil desde el campo "Name:" de la respuesta. El ataque suele pedir a los usuarios ejecutar el comando desde el cuadro Ejecutar de Windows, lo que permite descargar y ejecutar la segunda etapa del malware directamente desde la respuesta DNS, dificultando su detección.

Respuesta de consulta DNS que contiene el segundo comando de PowerShell a ejecutar
Fuente: Microsoft

Aunque el servidor malicioso ya no está activo, Microsoft informó que el comando de segunda etapa en PowerShell descargaba más malware desde infraestructura controlada por los atacantes.

El ataque terminaba descargando un archivo ZIP con un entorno de ejecución de Python y scripts maliciosos que realizaban reconocimiento del sistema y del dominio comprometido. Posteriormente, establecía persistencia mediante la creación de un VBScript en el directorio %APPDATA% y un acceso directo en la carpeta de inicio para ejecutarlo automáticamente al arrancar el sistema.

La carga final era **ModeloRAT**, un troyano de acceso remoto que permite a los atacantes controlar los equipos infectados.

A diferencia de campañas ClickFix anteriores (que solían usar HTTP para recuperar cargas útiles) esta variante emplea DNS como canal de comunicación y entrega, lo que le permite modificar los scripts maliciosos dinámicamente y camuflarse dentro del tráfico DNS legítimo, dificultando su detección.

La Guerra Híbrida llega a la Nieve: El Sabotaje Ruso Frustrado en los Juegos de Milán-Cortina 2026

2026 no solo marcó el inicio de los XXV Juegos Olímpicos de Invierno en Milán y Cortina d'Ampezzo, sino que también se convirtió en el escenario de uno de los enfrentamientos digitales más tensos de la década.
Mientras los atletas se preparaban para la ceremonia de apertura, en las sombras de la red se libraba una batalla para evitar que el evento fuera saboteado antes de empezar. Italia, en un despliegue de ciberdefensa sin precedentes, logró neutralizar una ofensiva masiva coordinada desde territorio ruso.

El Ataque:
Según reveló el ministro de Relaciones Exteriores de Italia, Antonio Tajani, la ofensiva no fue un incidente aislado, sino una oleada coordinada de ataques de denegación de servicio (DDoS) que apuntó a infraestructuras críticas. Los atacantes buscaron saturar los servidores de aproximadamente 120 sitios web, con objetivos estratégicos que incluían:

- Sedes Diplomáticas: La embajada italiana en Washington fue la primera en detectar la intrusión, seguida de consulados en Sídney, Toronto y París.
- Logística Olímpica: El ataque se centró con saña en los hoteles de Cortina d'Ampezzo, la joya de los Alpes donde se hospedan atletas y delegaciones internacionales. El objetivo era claro: desestabilizar la logística, bloquear las reservas y generar un clima de caos e inseguridad.
- Instituciones Académicas: Incluso la Universidad de La Sapienza en Roma se vio afectada, demostrando que la intención era golpear el corazón administrativo y educativo del país anfitrión.

¿Quiénes están detrás?

El grupo de hackers prorrusos NoName057 se adjudicó la autoría a través de sus canales de Telegram.

Utilizando un lenguaje beligerante, el grupo describió sus ataques como "misiles DDoS" y lanzó una advertencia directa al gobierno de Giorgia Meloni
El motivo declarado fue la venganza geopolítica. El grupo afirmó que el sabotaje era una respuesta directa al apoyo militar y diplomático de Italia a Ucrania. "La política de apoyo a los terroristas ucranianos será castigada con nuestros ataques", declararon los hackers, subrayando que cualquier nación que respalde a Kiev será considerada un objetivo legítimo en su guerra digital.

Más Información

Cómo proteger a las organizaciones durante los Juegos Olímpicos de Invierno, según los CISO

1. La Amenaza: El Abuso de la Confianza

Los expertos coinciden en que el mayor riesgo no son los virus nuevos, sino el uso indebido de accesos legítimos.

- Identidades Comprometidas: Los atacantes roban credenciales, sesiones o tokens para operar dentro de la red durante semanas sin ser detectados.
- Presión Operativa: Durante el evento, se elevan los niveles de acceso y se prioriza la disponibilidad sobre la seguridad, lo que facilita el abuso de aplicaciones y APIs.
- Deepfakes y Urgencia: La IA permite estafas sofisticadas (como videoconferencias falsas). Los empleados son más vulnerables porque esperan solicitudes "inusuales y urgentes" debido a la naturaleza del evento.

2. Riesgos para Aficionados y Organizaciones

- Fraude en Entradas: Los estafadores crean sitios espejo para robar datos bancarios. No solo es una pérdida de dinero, sino un compromiso de identidad a largo plazo.
- Datos Sensibles: El repositorio de información de asistentes y diplomáticos es un objetivo prioritario que debe protegerse incluso años después de clausurados los Juegos.

3. Estrategias de Protección (Consejos de CISO)

Para mitigar estos riesgos, las organizaciones deben enfocarse en tres pilares:

- Visibilidad en Tiempo Real: Monitorear cómo se usan las aplicaciones y APIs para detectar patrones anormales y detener el abuso automatizado antes de que cause daños.
- Higiene Digital Estricta: * No realizar transacciones personales (compras de entradas o mercancía) con cuentas de trabajo.
  - No instalar aplicaciones desde enlaces publicitarios o correos sospechosos.
- Cultura de Verificación: Recordar que "si algo parece demasiado bueno para ser verdad, probablemente sea una estafa". La capacitación en concienciación es el activo más fuerte.

Más Información

Vulnerabilidades destacadas

CVE-2025-21298

Microsoft

Vulnerabilidad de ejecución remota de código OLE de Windows

CVE-2025-21198

Microsoft

Vulnerabilidad de ejecución remota de código del paquete de computación de alto rendimiento (HPC) de Microsoft

CVE-2025-71155

Linux

En el kernel de Linux, se ha resuelto la siguiente vulnerabilidad: KVM: s390: Se ha corregido gmap_helper_zap_one_page(). Faltaban algunas comprobaciones en gmap_helper_zap_one_page(), lo que puede provocar daños en la memoria del invitado en determinadas circunstancias.

Más Información

Ciber incidentes en Colombia y en el mundo

ciberseguridad en Colombia y la región

En la última semana, el panorama de ciberseguridad en Colombia y la región mostró un incremento en la explotación de vulnerabilidades críticas, la distribución de troyanos de acceso remoto (RAT) a través de campañas de phishing, y ataques visibles como ransomware contra empresas y defacement en portales institucionales.

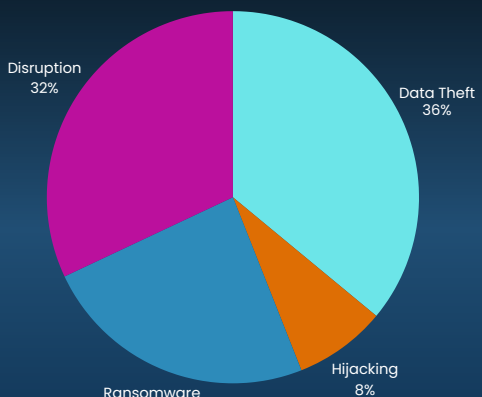
A nivel regional, también se observaron campañas de actores como Thegentlemen, AlphaLocker, LunaLock y Spacebears, lo que refleja la diversificación de amenazas. Este panorama evidencia una tendencia hacia ataques más sofisticados, potenciados incluso por el uso de inteligencia artificial, lo que obliga a reforzar controles técnicos en correo, servidores web y endpoints, así como fortalecer la concienciación del personal para anticipar impactos operativos y reputacionales en las organizaciones.

Más Información

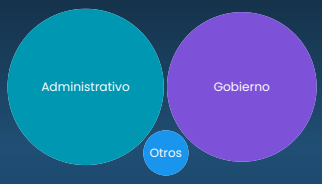
El mundo

24
Ciber incidentes

TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS

Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

www e-dea.co